n

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-082043
(43)Date of publication of application : 21.03.2000

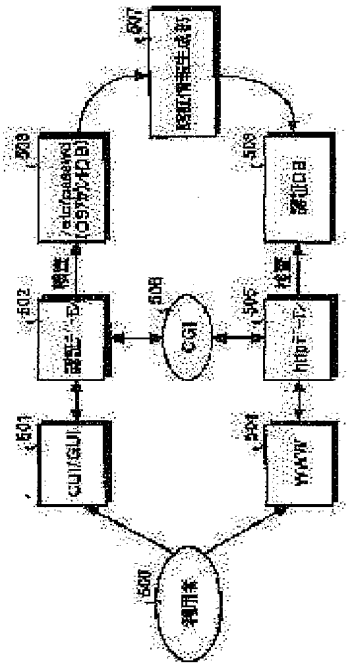
(51)Int.Cl. G06F 15/00

(21)Application number : 10-252459
(22)Date of filing : 07.09.1998

(71)Applicant : RICOH CO LTD
(72)Inventor : KAWAKAMI KAZUHIRO

(54) USER AUTHENTICATION SYSTEM, METHOD THEREFOR AND COMPUTER-READABLE RECORDING MEDIUM RECORDED WITH PROGRAM ALLOWING COMPUTER TO IMPLEMENT THE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To easily, speedily, and securely perform user authentication by systems.
SOLUTION: This system is provided with an OS account DB 503 which stores OS account information including a log-in name and a password, an authentication demon 502 which authenticates a user by using the OS account information stored in the OS account DB 503, an authentication information generation part 507 which generates user authentication information according to the OS account information stored in the OS account DB 503, an authentication DB 508 generated by the authentication information generating means 507, and a http demon 505 which authenticates the user by using the user authentication information stored in the authentication DB 508.



LEGAL STATUS

[Date of request for examination] 05.11.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－82043
（P2000－82043A）
(43)公開日　平成12年３月21日(2000.3.21)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード*（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ　５Ｂ０８５

審査請求　未請求　請求項の数11　ＯＬ　（全 16 頁）

(21)出願番号　特願平10－252459

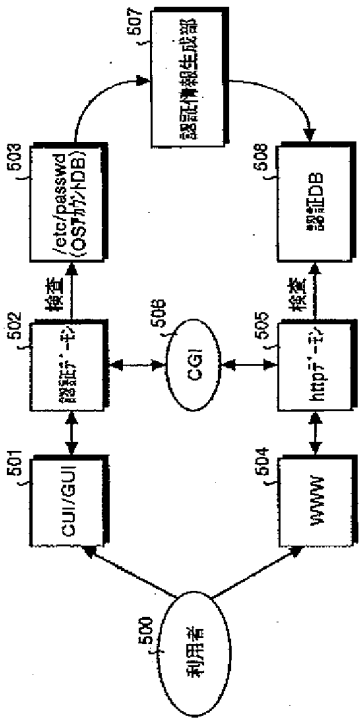
(22)出願日　平成10年９月７日(1998.9.7)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　川上　和博
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100104190
弁理士　酒井　昭徳

Ｆターム(参考)　5B085 AA08 AC03 AE01 BC01 BG07

(54)【発明の名称】　利用者認証システム、利用者認証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　システムごとの利用者認証を容易、迅速、かつ確実におこなうことを課題とする。
【解決手段】　ログイン名およびパスワードを含むＯＳアカウント情報を格納するＯＳアカウントＤＢ５０３と、ＯＳアカウントＤＢ５０３により格納されたＯＳアカウント情報を用いて利用者の認証をおこなう認証デーモン５０２と、ＯＳアカウントＤＢ５０３により格納されたＯＳアカウント情報に基づいて、利用者認証情報を生成する認証情報生成部５０７と、認証情報生成手段５０７により生成された認証ＤＢ５０８と、認証ＤＢ５０８により格納された利用者認証情報を用いて利用者の認証をおこなうｈｔｔｐデーモン５０５とを備える。



1

【特許請求の範囲】

【請求項１】　ログイン名およびパスワードを含むＯＳアカウント情報を格納するＯＳアカウント情報格納手段と、

前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報を用いて利用者の認証をおこなう第１認証手段と、

前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報に基づいて、利用者認証情報を生成する生成手段と、

前記生成手段により生成された利用者認証情報を格納する利用者認証情報格納手段と、

前記利用者認証情報格納手段により格納された利用者認証情報を用いて利用者の認証をおこなう第２認証手段と、

を備えたことを特徴とする利用者認証システム。

【請求項２】　前記第１認証手段または前記第２の認証手段のいずれかを選択する選択手段を備え、

前記選択手段により選択された認証手段により認証をおこなうことを特徴とする請求項１に記載の利用者認証システム。

【請求項３】　前記選択手段は、

複数の認証手段が選択可能である場合、前記第１認証手段を選択することを特徴とする請求項２に記載の利用者認証システム。

【請求項４】　前記第１の認証手段および／または前記第２の認証手段は、

前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報または利用者認証情報格納手段により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうことを特徴とする請求項１に記載の利用者認証システム。

【請求項５】　前記第１の認証手段および／または前記第２の認証手段は、

前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報を用いることができないとき、前記利用者認証情報格納手段により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうことを特徴とする請求項４に記載の利用者認証システム。

【請求項６】　ログイン名およびパスワードを含むＯＳアカウント情報を格納するＯＳアカウント情報格納工程と、

前記ＯＳアカウント情報格納工程により格納されたＯＳアカウント情報を用いて利用者の認証をおこなう第１認証工程と、

前記ＯＳアカウント情報格納工程よりに格納されたＯＳアカウント情報に基づいて、利用者認証情報を生成する生成工程と、

前記生成工程により生成された利用者認証情報を格納する利用者認証情報格納工程と、

2

前記利用者認証情報格納工程により格納された利用者認証情報を用いて利用者の認証をおこなう第２認証工程と、

を含んだことを特徴とする利用者認証方法。

【請求項７】　前記第１認証工程により認証をおこなうかまたは前記第２の認証工程により認証をおこなうかを選択する選択工程を含み、

前記選択工程により選択された認証工程により認証をおこなうことを特徴とする請求項６に記載の利用者認証方法。

【請求項８】　前記選択工程は、

複数の認証工程により認証することが選択可能である場合、前記第１認証工程により認証するよう選択することを特徴とする請求項７に記載の利用者認証方法。

【請求項９】　前記第１認証工程および／または前記第２認証工程は、

前記ＯＳアカウント情報格納工程により格納されたＯＳアカウント情報または利用者認証情報格納工程により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうことを特徴とする請求項６に記載の利用者認証方法。

【請求項１０】　前記第１認証工程および／または前記第２認証工程は、

前記ＯＳアカウント情報格納工程により格納されたＯＳアカウント情報を用いることができないとき、前記利用者認証情報格納工程により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうことを特徴とする請求項９に記載の利用者認証方法。

【請求項１１】　前記請求項６～１０に記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、図書館情報管理システム等のシステムを利用する利用者の認証をおこなう利用者認証システム、利用者認証方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【０００２】

【従来の技術】従来の利用者認証システムについて図１４を用いて説明する。図１４において、１４０１は、利用者ＩＤ、ログイン名、パスワードの入力、認証結果の表示等をおこなうキャラクター・ユーザー・インターフェイス／グラフィカル・ユーザー・インターフェイス（ＣＵＩ／ＧＵＩ）であり、１４０２は、認証処理を司る制御部である認証デーモンであり、１４０３は、オペレーション・システム（ＯＳ）を利用する際のＯＳアカウント情報を格納する／ｅｔｃ／ｐａｓｓｗｄ（ＯＳア

カウントＤＢ）である。

【０００３】また、１４０４は、ワールド・ワイド・ウェブ（WWW）であり、１４０５は、ハイパー・テキスト・トランスファー・プロトコル（ｈｔｔｐ）デーモンであり、１４０６は、コモン・ゲートウエイ・インターフェイス（ＣＧＩ）であり、１４０７はｈｔｔｐパスワード・データベース（ＤＢ）である。

【０００４】システム全体のＯＳを用いた或るシステム、たとえば、図書館情報管理システムを利用するための認証を要求する際、利用者１４００は、ＣＵＩ／ＧＵＩ１４０１に対して、ログイン名とパスワードを入力する。ログイン名とは、上記或るシステムを含むシステム全体のＯＳ使用を使用する際、登録により与えられる個人のアカウント情報である。

【０００５】ＣＵＩ／ＧＵＩ１４０１は、ログイン名が入力された場合は、その入力されたログイン名をパスワードとともに認証デーモン１４０２へ渡す。認証デーモン１４０２は、／ｅｔｃ／ｐａｓｓｗｄ（ＯＳアカウントＤＢ）１４０３に上記ログイン名およびパスワードを渡し、／ｅｔｃ／ｐａｓｓｗｄ（ＯＳアカウントＤＢ）１４０３にあらかじめ登録されているログイン名およびパスワードと照合し、両者が一致するか否かを検査することにより認証の判定をおこなう。

【０００６】一方、システム全体のＯＳを用いた或るシステムを利用するための認証を要求する際、利用者１４００は、ＣＵＩ／ＧＵＩ１４０１ではなく、ＷＷＷ１４０４に対して、ログイン名とパスワードを入力することもできる。

【０００７】この場合、ＷＷＷ１４０４は、ログイン名が入力された場合は、その入力されたログイン名をパスワードとともにｈｔｔｐデーモン１４０５へ渡す。ｈｔｔｐデーモン１４０５は、ｈｔｔｐパスワード・データベース（ＤＢ）１４０７１４０７に上記ログイン名およびパスワードを渡し、ｈｔｔｐパスワードＤＢ１４０７にあらかじめ登録されているログイン名およびパスワードと照合し、両者が一致するか否かを検査することにより認証の判定をおこなう。その後、ｈｔｔｐデーモンは、ＣＧＩ１４０６を通じて、システム全体のＯＳとのデータの通信をおこなう。

【０００８】このように、従来の利用者認証システムは、図書館情報管理システム等の或るシステムの利用をするための認証をする際、通常、システム全体のＯＳのアカウントＤＢを利用しておこなわれ、システム全体のＯＳのアカウント情報であるログイン名に対するパスワードが正しいかを検査し、正しい場合は、利用するシステムの許可を与えていた。

【０００９】

【発明が解決しようとする課題】しかしながら、上記の従来技術にあっては、ｈｔｔｐパスワードＤＢ１４０７に認証用ファイルを作成するおよび作成したファイルを管理することはシステム管理者にとって煩雑であるとともに、ｈｔｔｐパスワードＤＢをシステム全体のＯＳのＯＳアカウントＤＢ１４０３と同期をとることがきわめて困難であるため、確実に認証をおこなう際の障害になるという問題点があった。

【００１０】また、混雑や故障等により、ＯＳアカウントＤＢ１４０３により認証処理ができない状況になった場合に、システムの利用ができなくなるという問題点があった。

【００１１】特に、図書閲覧システムを含む図書館情報管理システムの場合、図書館を利用する利用者数は膨大な数となるため、すべての利用者に対するログイン名をアカウントＤＢに登録し管理することを想定すると、この問題は顕著なものとなる。

【００１２】この発明は、上述した従来例による問題点を解決するため、容易、迅速、かつ確実に利用者認証をおこなうことができる利用者認証システム、利用者認証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【００１３】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項１の発明に係る利用者認証システムは、ログイン名およびパスワードを含むＯＳアカウント情報を格納するＯＳアカウント情報格納手段と、前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報を用いて利用者の認証をおこなう第１認証手段と、前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報に基づいて、利用者認証情報を生成する生成手段と、前記生成手段により生成された利用者認証情報を格納する利用者認証情報格納手段と、前記利用者認証情報格納手段により格納された利用者認証情報を用いて利用者の認証をおこなう第２認証手段と、を備えたことを特徴とする。

【００１４】また、請求項２の発明に係る利用者認証システムは、請求項１の発明において、前記第１認証手段または前記第２の認証手段のいずれかを選択する選択手段を備え、前記選択手段により選択された認証手段により認証をおこなうことを特徴とする。

【００１５】また、請求項３の発明に係る利用者認証システムは、請求項２の発明において、前記選択手段が、複数の認証手段が選択可能である場合、前記第１認証手段を選択することを特徴とする。

【００１６】また、請求項４の発明に係る利用者認証システムは、請求項１の発明において、前記第１の認証手段および／または前記第２の認証手段が、前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報または利用者認証情報格納手段により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうことを特徴とする。

【００１７】また、請求項５の発明に係る利用者認証システムは、請求項４の発明において、前記第１の認証手段および／または前記第２の認証手段が、前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報を用いることができないとき、前記利用者認証情報格納手段により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうことを特徴とする。

【００１８】また、請求項６の発明に係る利用者認証方法は、ログイン名およびパスワードを含むＯＳアカウント情報を格納するＯＳアカウント情報格納工程と、前記ＯＳアカウント情報格納工程により格納されたＯＳアカウント情報を用いて利用者の認証をおこなう第１認証工程と、前記ＯＳアカウント情報格納工程よりに格納されたＯＳアカウント情報に基づいて、利用者認証情報を生成する生成工程と、前記生成工程により生成された利用者認証情報を格納する利用者認証情報格納工程と、前記利用者認証情報格納工程により格納された利用者認証情報を用いて利用者の認証をおこなう第２認証工程と、を含んだことを特徴とする。

【００１９】また、請求項７の発明に係る利用者認証方法は、請求項６の発明において、前記第１認証工程により認証をおこなうかまたは前記第２の認証工程により認証をおこなうかを選択する選択工程を含み、前記選択工程により選択された認証工程により認証をおこなうことを特徴とする。

【００２０】また、請求項８の発明に係る利用者認証方法は、請求項７の発明において、前記選択工程が、複数の認証工程により認証することが選択可能である場合、前記第１認証工程により認証するよう選択することを特徴とする。

【００２１】また、請求項９の発明に係る利用者認証方法は、請求項６の発明において、前記第１認証工程および／または前記第２認証工程が、前記ＯＳアカウント情報格納工程により格納されたＯＳアカウント情報または利用者認証情報格納工程により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうことを特徴とする。

【００２２】また、請求項１０の発明に係る利用者認証方法は、請求項９の発明において、前記第１認証工程および／または前記第２認証工程が、前記ＯＳアカウント情報格納工程により格納されたＯＳアカウント情報を用いることができないとき、前記利用者認証情報格納工程により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうことを特徴とする。

【００２３】また、請求項１１の発明に係る記憶媒体は、請求項６～１０に記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムを機械読み取り可能となり、これによって、請求項６～１０の動作をコンピュータによって実現することが可能である。

【００２４】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る利用者認証システム、利用者認証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【００２５】（実施の形態１）まず、この発明の実施の形態１による利用者認証システムを含む図書館情報管理システム全体の構成を説明する。図１は、この発明の実施の形態１による利用者認証システムを含む図書館情報管理システム全体の構成を示す説明図である。図１において、図書館情報管理システムは、学術情報センター１００と、図書館１１０と、サテライトライブラリ１２０と、事務室１３０と、計算機演習室１４０と、研究室１５０とがそれぞれ、専用回線あるいはインターネット等のネットワークで接続されている。

【００２６】図書館１１０には、データ入力装置であるワークステーション（ＷＳ）１１１およびパーソナルコンピュータ（ＰＣ）１１２が、図書管理サーバー１１３および図書検索サーバー１１４に接続されている。その他、スキャナ１１５およびプリンタ１１６が同様にネットワークで接続されている。また、図書管理サーバー１１３は業務用データベース１１７を備えており、また、図書検索サーバー１１４は検索用データベース１１８を備えている。また、図書管理サーバー１１３および図書検索サーバー１１４をデータ入力装置とすることもできる。

【００２７】また、サテライトライブラリ１２０、事務室１３０、計算機演習室１４０、研究室１５０には、データ入力装置であるＷＳ１２１，１４１，１５１、あるいは、ＰＣ１３２，１４２，１５２がそれぞれ備えられている。

【００２８】また、実施の形態１では、図書管理サーバー１１３と図書検索サーバー１１４とは別個の構成としたが、システム全体の規模等に応じて共用のサーバーとして運用するようにしてもよい。

【００２９】図２は、実施の形態１による図書館情報管理システムの各サブシステムと図書館情報管理の業務との関係を示す説明図である。図２において、図書館情報管理システムは、目録管理を中心とした基本システム２００と、図書検索システム２０１と、閲覧管理システム２０２と、発注受入システム２０３と、雑誌管理システム２０４と、蔵書点検システム２０５と、相互貸借システム２０６の６つのサブシステムから構成される。

【００３０】基本システム２００は、図書や雑誌の目録や所在を管理するためのシステムである。書誌データ、所蔵データの登録や修正、削除等をおこなうことにより、目録作成業務２５１を実行する。また、学術情報セ

ンター１００が提供する目録システム（ＣＡＴ）へ書誌情報を登録したり、学術情報センターに登録されている情報をローカルデータベースへ登録することにより、ＣＡＴの利用業務２５２を実行する。さらに、図書館１１０内の図書の配架処理に関する配架業務２５３を実行する。

【００３１】図書検索システム２０１は、図書館１１０内の端末（ＷＳ１１１、ＰＣ１１２）や、図書館１１０外の端末（ＷＳ１２１，１４１，１５１、ＰＣ１３２，１４２，１５２）から、図書や雑誌の書誌、所在、状態を検索・照合するためのシステムである。この図書館検索システム２０１には、たとえば、ＯＰＡＣ（Ｏｎｌｉｎｅ　Ｐｕｂｌｉｃ　Ａｃｃｅｓｓ　Ｃａｔａｌｏｇｕｅ）が用いられる。

【００３２】また、図書館検索システム２０１のインターフェイスには、キャラクター・ユーザー・インターフェイス（ＣＵＩ）、グラフィカル・ユーザー・インターフェイス（ＧＵＩ）、ワールド・ワイド・ウェブ（ＷＷＷ）を用いることができ、これらにより、利用者による目録検索業務２５４を実行する。

【００３３】閲覧管理システム２０２は、貸出返却や予約管理、延滞処理、利用者管理、利用統計等の閲覧に関する管理をするためのシステムである。これにより、貸出返却業務２５５、図書予約業務２５６、利用者管理業務２５７を実行する。

【００３４】発注受入システム２０３は、購入依頼の受付から、重複チェック、予算チェック、発注受入、未納品チェックまで、図書（単行書）の発注受入をおこなうためのシステムである。これにより、購入調査業務２５８、発注業務２５９、受入業務２６０を実行する。

【００３５】雑誌管理システム２０４は、図書館１１０で購入している雑誌や逐次刊行物の発注受入や契約管理、ならびに製本業務をおこなうためのシステムである。これにより、雑誌や逐次刊行物の購入調査業務２５８、発注業務２５９、受入業務２６０、さらには、製本業務２６１を実行する。

【００３６】蔵書点検システム２０５は、図書館１１０が管理している図書資料の所在点検業務をおこなうためのシステムである。ハンディターミナル等を利用して、所在単位、書架単位で点検をおこなう。また、長期貸出者への所在調査票の出力もおこなう。これにより、蔵書点検業務２６２を実行する。

【００３７】相互貸借システム２０６は、学術情報センター１００の図書館間相互貸借（ＩＬＬ）の受付・依頼情報をデータベースで管理するためのシステムである。文献複写や現物貸借に使用する各種の作業表の出力もおこなう。これにより、ＩＬＬによる貸借業務２６３を実行する。

【００３８】つぎに、図書館情報管理システムのデータベースの構造について説明する。図３は、本実施の形態による図書館情報管理システムのデータベースの構成を示す説明図である。図３において、図書館情報管理システムのデータベースは、業務用データベース１１７と、検索用データベース１１８と、さらに、サブシステム２０１～２０６間に共通のコード表３１０が格納されたコードマスターデータベース３００とから構成される。

【００３９】業務用データベース１１７は、主に図書館の職員が使うデータベースであり、図書館の職員が業務で作成、変更するデータは、すべて業務用データベース１１７に登録される。

【００４０】業務用のデータベースには、購入依頼・発注受入データベース３０１と、雑誌管理データベース３０２と、目録（書誌、所蔵）データベース３０３と、所蔵点検・点検履歴データベース３０４と、貸出返却・貸出予約・利用者データベース３０５と、相互貸借・集計データベース３０６とを含む構造となっている。

【００４１】購入依頼・発注受入データベース３０１は、発注受入システム２０３が利用するデータベースである。また、雑誌管理データベース３０２は、雑誌管理システム２０４が利用するシステムであり、雑誌管理とはたとえば雑誌の契約、発注、受入等である。また、目録（書誌、所蔵）データベース３０３は、発注受入システム２０３、雑誌管理システム２０４、目録管理システム２００、蔵書点検システム２０５、閲覧管理システム２０２が利用するシステムである。

【００４２】所蔵点検・点検履歴データベース３０４は、蔵書点検システム２０５が利用するシステムであり、貸出返却・貸出予約・利用者データベース３０５は、蔵書点検システム２０５、閲覧管理システム２０２が利用するシステムであり、相互貸借・集計データベース３０６は、相互貸借システム２０６が利用するシステムである。

【００４３】また、検索用データベース１１８は、一般利用者が検索する際、参照するデータベースであり、図書雑誌検索データベース３０７が格納されている。検索するときに必要なのは、図書や雑誌の書誌と所蔵のデータであり、そのため、検索に必要なデータだけを業務用データベース１１７の中から取り出して、効率よく検索ができるデータの形式にして登録している。

【００４４】つぎに、利用者認証システムを実現する図書管理サーバー１１３または図書検索サーバー１１４のハードウエア構成について説明する。図４は、実施の形態１による利用者認証システムのハードウエア構成を示すブロック図である。

【００４５】図４において、４０１はシステム全体を制御するＣＰＵを、４０２はブートプログラムを記憶したＲＯＭを、４０３はＣＰＵのワークエリアとして使用されるＲＡＭを、４０４はＣＰＵ４０１の制御にしたがってＨＤ（ハードディスク）４０５に対するデータのリード／ライトを制御するＨＤＤ（ハードディスクドライ

ブ）を、４０５はＨＤＤ４０４の制御で書き込まれたデータを記憶するＨＤを、４０６はＣＰＵ４０１の制御にしたがってＦＤ（フロッピーディスク）４０７に対するデータのリード／ライトを制御するＦＤＤ（フロッピーディスクドライブ）を、４０７はＦＤＤ４０６の制御で書き込まれたデータを記憶する着脱自在のＦＤを、４０８は文字、画像等を含むドキュメントや機能情報等を表示するディスプレイをそれぞれ示している。

【００４６】また、４０９は通信回線４１０を介してネットワークＮＥＴに接続され、そのネットワークＮＥＴと内部のインターフェイスを司るインターフェイス（Ｉ／Ｆ）を、４１１は文字、数値、各種指示等の入力のためのキーを備えたキーボードを、４１２はカーソルの移動や範囲選択等をおこなうマウスを、４１３はＯＣＲ機能を含み、画像を光学的に読み取るスキャナを、４１４は、図書やカード等に付与（印刷）されたバーコードを読み取るバーコードリーダを、４１５はドキュメントやバーコード等を印刷するプリンタを、４１６は上記各部を接続するためのバスをそれぞれ示している。また、バス４１６は業務用データベース１１７にも接続されている。

【００４７】また、図書検索サーバー１１４のハードウエア構成は、図書管理サーバー１１３のハードウエア構成とは、データベースが業務用データベース１１７であるか検索用データベース１１８であるかの違いをのぞき、その他はすべて同様であるので、その説明は省略する。さらに、本実施の形態では、図書管理サーバー１１３と図書検索サーバー１１４とは別個の構成としたが、システム全体の規模等に応じて共用のサーバーとして運用するようにしてもよい。

【００４８】つぎに、実施の形態１による利用者認証システムの機能的な構成について説明する。図５は、実施の形態１による利用者認証システムの構成を示す機能ブロック図である。図５において、利用者認証システムは、キャラクター・ユーザー・インターフェイス（ＣＵＩ）／グラフィカル・ユーザー・インターフェイス（ＧＵＩ）５０１と、認証デーモン５０２と、／ｅｔｃ／ｐａｓｓｗｄ（ＯＳアカウントデータベース（ＤＢ））５０３と、ワールド・ワイド・ウェブ（ＷＷＷ）５０４と、ハイパー・テキスト・トランスファー・プロトコル（ｈｔｔｐ）デーモン５０５と、コモン・ゲートウエイ・インターフェイス（ＣＧＩ）５０６と、認証情報生成部５０７と、認証データベース（ＤＢ）５０８とを含む構成となっている。

【００４９】また、通常、ワールド・ワイド・ウェブ（ＷＷＷ）５０４と、ｈｔｔｐデーモン５０５と、コモン・ゲートウエイ・インターフェイス（ＣＧＩ）５０６と、認証データベース（ＤＢ）５０８とにより、ＷＷＷサーバーが構成される。

【００５０】ＣＵＩ／ＧＵＩ５０１は、認証を要求する際、利用者がログイン名およびパスワードを入力するものである。また、ＣＵＩ／ＧＵＩ５０１は、認証結果を表示する。

【００５１】認証デーモン５０２は、利用者認証処理を司る制御部であり、ＯＳアカウントＤＢ５０３により格納されたログイン名およびパスワードとＣＵＩ／ＧＵＩ５０１により入力されたログイン名およびパスワードが一致するか否かを判断することにより利用者認証をおこなうものである。

【００５２】／ｅｔｃ／ｐａｓｓｗｄ（ＯＳアカウントデータベース（ＤＢ））５０３は、ＯＳのアカウント情報であるログイン名およびパスワード等のＯＳのアカウント情報を格納する。

【００５３】ワールド・ワイド・ウェブ（ＷＷＷ）５０４は、インターネットで用いる情報検索システムの一つである。ＷＷＷブラウザ等を用いることにより、データの入力および表示をすることができる。

【００５４】ｈｔｔｐデーモン５０５は、ｈｔｔｐによって利用者認証処理を含むデータ処理を司る制御部であり、ＣＧＩ５０６とのデータの受渡しおよび認証ＤＢ５０８により格納されたアカウント情報とＷＷＷ５０４により入力されたアカウント情報とが一致するか否かを判断することにより利用者認証をおこなうものである。

【００５５】コモン・ゲートウエイ・インターフェイス（ＣＧＩ）５０６は、ＷＷＷサーバーから外部プログラムであるゲートウエイを呼び出して処理を依頼し、処理結果をＷＷＷ（ブラウザ）５０４に送信する。

【００５６】認証情報生成部５０７は、ＯＳアカウントＤＢに格納されている情報に基づいて、認証ＤＢ５０８に格納する認証情報を生成する。具体的には、システム運転停止時や利用者の少ない夜間に、ＯＳアカウントＤＢからアカウント情報をコピーすることにより、ＷＷＷサーバー用である認証ＤＢに格納する認証情報を生成する。また、認証データベース（ＤＢ）５０８は、認証情報生成部５０７により生成された認証情報を格納する。

【００５７】利用者５００は、２つの方法により利用者認証をおこなうことができる。一つの方法は、認証を要求する際、ログイン名およびパスワード等のアカウント情報をＣＵＩ／ＧＵＩ５０１に入力する。ＣＵＩ／ＧＵＩ５０１は、入力されたログイン名およびパスワードを認証デーモン５０２に渡す。認証デーモン５０２は、通常、渡されたログイン名およびパスワードを、ＯＳアカウントＤＢ５０３へ渡して、ＯＳアカウントＤＢ５０３にあらかじめ登録されているログイン名およびパスワードと照合し、両者が一致するか否かを検査することにより認証の判定をおこなうものである。これは、従来のＷＷＷ５０４を使用しない場合の認証方法である。

【００５８】一方、もう一つの方法は、認証を要求する際、ログイン名およびパスワード等のアカウント情報をＷＷＷ５０４に入力する。ＷＷＷ５０４は、入力された

ログイン名およびパスワードをｈｔｔｐデーモン５０５に渡す。ｈｔｔｐデーモン５０５は、ＯＳアカウントＤＢ５０３とは別個に設けられた認証ＤＢ５０８を用いて、ログイン名およびパスワードの照合をおこない、両者が一致するか否かを検査することにより認証の判定をおこなうものである。これにより、ＣＧＩ５０６および認証デーモン５０２を介してＯＳアカウントＤＢに依存することなく、利用者認証をおこなうことができる。

【００５９】つぎに、利用者認証システムの認証情報生成部５０７による認証情報の生成処理の内容について説明する。図６は、実施の形態１による利用者認証システムの認証情報生成処理の手順を示すフローチャートである。

【００６０】図６のフローチャートにおいて、まず、認証情報を生成する日時をあらかじめ設定する。日時としては、たとえば、毎日あるいは所定日数ごとの夜間の所定の時間としてもよく、また、システム運用を停止する日時等としてもよい。

【００６１】そして、あらかじめ定められた所定日時となったか否かを判断する（ステップＳ６０１）。ここで、所定日時となるのを待って、所定日時となった場合（ステップＳ６０１肯定）は、つぎに、コピー元のＯＳアカウントＤＢ５０３のアカウント情報の更新があったか否かを判断する（ステップＳ６０２）。ここで、更新がなかった場合（ステップＳ６０２否定）は、アカウント情報のコピーをする必要がないので、ステップＳ６０１へ移行し、再度、所定の日時になるのを待つ。

【００６２】一方、ステップＳ６０２において、情報の更新があった場合（ステップＳ６０２肯定）は、認証情報の生成をおこなう（ステップＳ６０３）。具体的には、ＯＳアカウントＤＢ５０３の所定のアカウント情報をコピーすることによりおこなう。

【００６３】つぎに、コピーされたアカウント情報を認証ＤＢ５０８に格納する（ステップＳ６０７）。これにより認証情報の生成処理は終了し、ステップＳ６０１へ移行し、再度、所定の日時になるのを待つ。

【００６４】つぎに、実施の形態１による利用者認証システムの認証処理の内容について説明する。図７は、実施の形態１による利用者認証システムの認証処理の一連の手順を示すフローチャートである。

【００６５】図７のフローチャートにおいて、まず、ＷＷＷ５０４にログイン名が入力されたか否かを判断する（ステップＳ７０１）。ここで、ログイン名が入力されるのを待って、ログイン名が入力された場合（ステップＳ７０１肯定）は、つぎに、パスワードが入力されたか否かを判断する（ステップＳ７０２）。

【００６６】ステップＳ７０２においても、ステップＳ７０１と同様に、パスワードが入力されるのを待って、パスワードが入力された場合（ステップＳ７０２肯定）は、ステップＳ７０１において入力されたログイン名とステップＳ７０２において入力されたパスワードをｈｔｔｐデーモン５０５に渡す（ステップＳ７０３）。

【００６７】ログイン名とパスワードを渡されたｈｔｔｐデーモン５０５は、認証ＤＢ５０８を用いてログイン名およびパスワードの検査をおこなう（ステップＳ７０４）。検査の結果、ログイン名およびパスワードが認証ＤＢ５０８に格納されていたログイン名およびパスワードと一致するか否かを判断し（ステップＳ７０５）、不一致の場合（ステップＳ７０５否定）は、「ＮＧ（拒否）」を通知する（ステップＳ７０６）。その後、ステップＳ７０１へ移行し、再度のログイン名の入力を待つ。

【００６８】ステップＳ７０５において、ログイン名およびパスワードが認証者ＤＢ５０８にあらかじめ格納されていたログイン名およびパスワードと一致する場合（ステップＳ７０５肯定）は、「ＯＫ（承認）」を通知し（ステップＳ７０７）、その後、利用者５００に対して、認証要求があったシステムを利用可能な状態にし（ステップＳ７０８）、すべての処理を終了する。

【００６９】以上説明したように、実施の形態１によれば、認証情報生成部５０７により、ＯＳアカウント情報と同期した内容のＷＷＷサーバー用の認証情報を認証ＤＢ５０８内に生成するので、管理者に負担をかけることなく、システムのＯＳの認証と同様の認証をＷＷＷサーバー側でおこなうことができる。

【００７０】特に、複数のコンピュータシステムが任意の通信媒体を介して接続された分散環境において、特定のコンピュータシステムによって利用者情報を一元管理し、ログイン名およびパスワードにより利用者認証をおこない、分散環境上のサービスの利用を許可する利用者認証システムに対して有用である。

【００７１】（実施の形態２）さて、実施の形態１では、ＣＵＩ／ＧＵＩにより認証するか、ＷＷＷにより認証するかについては、認証をおこなう端末等によりあらかじめ定められていたが、以下に説明する実施の形態２のように、認証方式選択部により、いずれかの認証方式を選択できるようにしてもよい。

【００７２】この発明の実施の形態２による利用者認証システムを含む図書館情報管理システム全体の構成、図書館情報管理システムの各サブシステムと図書館情報管理の業務との関係、図書館情報管理システムのデータベースの構造、および利用者認証システムを実現する図書管理サーバー１１３、図書検索サーバー１１４のハードウエア構成については、実施の形態１の図１～図４において説明した内容と同様であるので、その説明は省略する。

【００７３】つぎに、実施の形態２による利用者認証システムの機能的な構成について説明する。図８は、実施の形態２による利用者認証システムの構成を示す機能ブロック図である。図８において、利用者認証システム

は、ＣＵＩ／ＧＵＩ８０１と、認証デーモン８０２と、ＯＳアカウントＤＢ８０３と、ＷＷＷ８０４と、ｈｔｔｐデーモン８０５と、ＣＧＩ８０６と、認証情報生成部８０７と、認証ＤＢ８０８と、さらに、認証方式選択部８１０とを含む構成になっている。

【００７４】ＣＵＩ／ＧＵＩ８０１、認証デーモン８０２、ＯＳアカウントＤＢ８０３、ＷＷＷ８０４、ｈｔｔｐデーモン８０５、ＣＧＩ８０６、認証情報生成部８０７、認証ＤＢ８０８は、実施の形態１における図５のＣＵＩ／ＧＵＩ５０１、認証デーモン５０２、ＯＳアカウントＤＢ５０３、ＷＷＷ５０４、ｈｔｔｐデーモン５０５、ＣＧＩ５０６、認証情報生成部５０７、認証ＤＢ５０８と同様の構成であるので、その説明は省略する。

【００７５】認証方式選択部８１０は、認証する際の２つの方式である、ＣＵＩ／ＧＵＩ８０１を用いるのか、あるいは、ＷＷＷ８０４を用いるのかを選択することできる。選択の方法として、両方の認証方式を利用できることを前提として、いずれかの利用方式を利用者が選択するものである。これにより、利用者が所望する認証方式を選択することが可能である。

【００７６】他の選択の方法として、あらかじめ認証方式に優先順位を付加しておき、その優先順位に基づいて、選択すべき認証方式を決定するものである。これにより、常に優先順位の高い認証方式が選択され、当該優先順位の高い認証方式による認証ができない場合に、つぎに優先順位の高い認証方式が選択されることにより、いずれかの認証方式に認証要求が集中しないようにすることができる。

【００７７】つぎに、実施の形態２による利用者認証システムの認証処理の内容について説明する。図９は、実施の形態２による利用者認証システムの認証処理の一連の手順を示すフローチャートである。

【００７８】図９のフローチャートにおいて、まず、利用者の認証する際、ＣＵＩ／ＧＵＩ８０１が選択されたか否かを判断する（ステップＳ９０１）。ここで、ＣＵＩ／ＧＵＩ８０１が選択されなかった場合（ステップＳ９０１否定）は、図７におけるステップＳ７０１へ移行し、ＷＷＷ８０４による認証がおこなわれる。

【００７９】一方、ステップＳ９０１において、ＣＵＩ／ＧＵＩ８０１が選択された場合（ステップＳ９０１肯定）は、つぎに、ＣＵＩ／ＧＵＩ８０１にログイン名が入力されたか否かを判断する（ステップＳ９０２）。ここで、ログイン名が入力されるのを待って、ログイン名が入力された場合（ステップＳ９０２肯定）は、つぎに、パスワードが入力されたか否かを判断する（ステップＳ９０３）。

【００８０】ステップＳ９０３においても、ステップＳ９０２と同様に、パスワードが入力されるのを待って、パスワードが入力された場合（ステップＳ９０３肯定）は、ステップＳ９０２において入力されたログイン名とステップＳ９０２において入力されたパスワードを認証デーモン８０２へ渡す（ステップＳ９０４）。

【００８１】ログイン名とパスワードを渡された認証デーモン８０２は、ＯＳアカウントＤＢ８０３を用いてログイン名およびパスワードの検査をおこなう（ステップＳ９０５）。検査の結果、ログイン名およびパスワードがＯＳアカウントＤＢ８０３にあらかじめ格納されていたログイン名およびパスワードと一致するか否かを判断し（ステップＳ９０６）、不一致の場合（ステップＳ９０６否定）は、「ＮＧ（拒否）」を通知する（ステップＳ９０７）。その後、ステップＳ９０１へ移行し、再度、認証方式が選択されるのを待つ。

【００８２】ステップＳ９０６において、ログイン名およびパスワードがＯＳアカウントＤＢ８０３にあらかじめ格納されていたログイン名およびパスワードと一致する場合（ステップＳ９０６肯定）は、「ＯＫ（承認）」を通知し（ステップＳ９０８）、その後、利用者８００に対して、認証要求があったシステムを利用可能な状態にし（ステップＳ９０９）、すべての処理を終了する。

【００８３】つぎに、実施の形態２による利用者認証システムの認証方式選択部８１０の選択処理の一例について説明する。図１０は、実施の形態２による利用者認証システムの認証方式選択部８１０の選択処理の手順を示すフローチャートである。

【００８４】図１０のフローチャートにおいて、まず、複数の認証方式が選択可能か否かを判断する（ステップＳ１００１）。ここで、複数の認証方式の選択が可能な場合（ステップＳ１００１肯定）は、あらかじめ定められた選択の優先順位に基づいて、たとえば、ＣＵＩ／ＧＵＩ８０１による認証方式を選択し、図９のステップＳ９０２へ移行する。

【００８５】一方、ステップＳ１００１において、複数の認証方式の選択が可能でない場合（ステップＳ１００１否定）は、つぎに、ＣＵＩ／ＧＵＩ８０１が選択可能であるか否かを判断する（ステップＳ１００２）。ここで、ＣＵＩ／ＧＵＩ８０１が選択可能である場合（ステップＳ１００２肯定）は、同じく図９のステップＳ９０２へ移行する。

【００８６】一方、ステップＳ１００２において、ＣＵＩ／ＧＵＩ８０１が選択可能でない場合（ステップＳ１００２否定）は、つぎに、ＷＷＷ８０４が選択可能であるか否かを判断する（ステップＳ１００３）。ここで、ＷＷＷ８０４が選択可能である場合（ステップＳ１００３肯定）は、実施の形態１における図７のステップＳ７０１へ移行する。

【００８７】一方、ステップＳ１００３において、ＷＷＷ８０４が選択可能でない場合（ステップ１００３否定）は、選択できる認証方式が存在しないため、現状においては利用者認証ができない旨を警告し（ステップＳ１００４）、選択処理を終了する。

【００８８】以上説明したように、実施の形態２によれば、利用者が所望する認証方式を選択することができる。また、優先順位の高い認証方式による認証ができない場合に、つぎに優先順位の高い認証方式が選択されることにより、いずれかの認証方式に認証要求が集中しないようにし、効率的に認証処理をおこなうことができる。

【００８９】また、複数の認証手段が選択可能な場合に、ＯＳアカウントＤＢ８０３のアカウント情報を用いて認証処理をおこなうため、認証処理をより迅速におこなうことができる。

【００９０】特に、複数のコンピュータシステムが任意の通信媒体を介して接続された分散環境において、特定のコンピュータシステムによって利用者情報を一元管理し、利用者ＩＤおよびパスワードにより利用者認証をおこない、分散環境上のサービスの利用を許可する利用者認証システムに対して有用である。

【００９１】（実施の形態３）さて、実施の形態１および２では、認証デーモンはＯＳアカウントＤＢを用いて認証をおこない、ｈｔｔｐデーモンは認証ＤＢを用いて認証をおこなっていたが、以下に説明する実施の形態３のように、認証デーモンがＯＳアカウントＤＢまたは認証ＤＢを選択的に用いることにより、認証処理をおこなうようにしてもよい。

【００９２】この発明の実施の形態３による利用者認証システムを含む図書館情報管理システム全体の構成、図書館情報管理システムの各サブシステムと図書館情報管理の業務との関係、図書館情報管理システムのデータベースの構造、および利用者認証システムを実現する図書管理サーバー１１３、図書検索サーバー１１４のハードウエア構成については、実施の形態１の図１～図４において説明した内容と同様であるので、その説明は省略する。

【００９３】つぎに、実施の形態３による利用者認証システムの機能的な構成について説明する。図１１は、実施の形態２による利用者認証システムの構成を示す機能ブロック図である。図１１において、利用者認証システムは、ＣＵＩ／ＧＵＩ１１０１と、認証デーモン１１０２と、ＯＳアカウントＤＢ１１０３と、ＷＷＷ１１０４と、ｈｔｔｐデーモン１１０５と、ＣＧＩ１１０６と、認証情報生成部１１０７と、認証ＤＢ１１０８を含む構成となっている。

【００９４】ここで、認証デーモン１１０２をのぞく、ＣＵＩ／ＧＵＩ１１０１、ＯＳアカウントＤＢ１１０３、ＷＷＷ１１０４、ｈｔｔｐデーモン１１０５、ＣＧＩ１１０６、認証情報生成部１１０７、認証ＤＢ１１０８は、実施の形態１における図５のＣＵＩ／ＧＵＩ７０１、ＯＳアカウントＤＢ７０３、ＷＷＷ７０４、ｈｔｔｐデーモン７０５、ＣＧＩ７０６、認証情報生成部７０７、認証ＤＢ７０８と同様の構成であるので、その説明は省略する。

【００９５】認証デーモン１１０２は、利用者認証処理を司る制御部であり、ＯＳアカウントＤＢ１１０３により格納されたログイン名およびパスワードとＣＵＩ／ＧＵＩ１１０１により入力されたログイン名およびパスワードが一致するか否かを判断することにより利用者認証をおこなうものである。

【００９６】また、認証デーモン１１０２は、認証ＤＢ１１０８により格納されたログイン名およびパスワードとＣＵＩ／ＧＵＩ１１０１により入力されたログイン名およびパスワードが一致するか否かを判断することにより利用者認証をおこなうこともできる。したがって、認証デーモン１１０２は、ＯＳアカウントＤＢ１１０３と認証ＤＢ１１０８を選択的に用いることができる。これにより、ＯＳアカウントＤＢ１１０３が使用不可能な状態となった場合等に、認証ＤＢ１１０８を用いて、迅速に認証をすることができる。

【００９７】ＯＳアカウントＤＢ１１０３または認証ＤＢ１１０８のいずれかを選択する方法としては、優先順位をあらかじめ設定し、優先順位の高いＤＢを選択する。ここで、優先順位の高いＤＢが利用可能な状態でない場合は、つぎに優先順位の高いＤＢを選択する。また、利用者１１００に所望のＤＢを選択させる方法や、乱数を発生させ、認証する都度、発生させた乱数に基づいてランダムにＤＢを選択する方法であってもよい。

【００９８】利用者１１００は、認証を要求する際、ログイン名およびパスワードをＣＵＩ／ＧＵＩ１１０１に入力する。ＣＵＩ／ＧＵＩ１１０１は、入力されたログイン名およびパスワードを認証デーモン１１０２に渡す。認証デーモン１１０２は、ＤＢを選択し、選択したＤＢへログイン名およびパスワードを渡して、上記ＤＢにあらかじめ登録されているログイン名およびパスワードと照合し、両者が一致するか否かを検査することにより認証の判定をおこなう。

【００９９】つぎに、実施の形態３による利用者認証システムの認証処理の内容について説明する。図１２は、実施の形態３による利用者認証システムの認証処理の手順を示すフローチャートである。

【０１００】図１２のフローチャートにおいて、まず、ＣＵＩ／ＧＵＩ１１０１にログイン名が入力されたか否かを判断する（ステップＳ１２０１）。ここで、ログイン名が入力されるのを待って、ログイン名が入力された場合（ステップＳ１２０１肯定）は、つぎに、パスワードが入力されたか否かを判断する（ステップＳ１２０２）。

【０１０１】ステップＳ１２０２においても、ステップＳ１２０１と同様に、パスワードが入力されるのを待って、パスワードが入力された場合（ステップＳ１２０２肯定）は、ステップＳ１２０１において入力されたログイン名とステップＳ１２０２において入力されたパスワ

ードを認証デーモン１１０２へ渡す（ステップＳ１２０３）。

【０１０２】つぎに、ＯＳアカウントＤＢ１１０３が選択されたか否かを判断する（ステップＳ１２０４）。ここで、ＯＳアカウントＤＢ１１０３が選択された場合（ステップＳ１２０４肯定）は、実施の形態２による図９のステップＳ９０５へ移行する。

【０１０３】一方、ステップＳ１２０４において、ＯＳアカウントＤＢ１１０３が選択されなかった場合（ステップＳ１２０４否定）は、認証ＤＢ１１０８を用いてログイン名およびパスワードの検査をおこなう（ステップＳ１２０５）。検査の結果、ログイン名およびパスワードが認証ＤＢ１１０８にあらかじめ格納されていたログイン名およびパスワードと一致するか否かを判断し（ステップＳ１２０６）、不一致の場合（ステップＳ１２０６否定）は、「ＮＧ（拒否）」を通知する（ステップＳ１２０７）。その後、ステップＳ１２０１へ移行し、再度のログイン名の入力を待つ。

【０１０４】ステップＳ１２０６において、ログイン名およびパスワードが上記選択されたＤＢにあらかじめ格納されていたログイン名およびパスワードと一致する場合（ステップＳ１２０６肯定）は、「ＯＫ（承認）」を通知し（ステップＳ１２０８）、その後、利用者１１００に対して、認証要求があったシステムを利用可能な状態にし（ステップＳ１２０９）、すべての処理を終了する。

【０１０５】つぎに、実施の形態３による利用者認証システムの認証デーモン１１０２のＤＢ選択処理の一例について説明する。図１３は、実施の形態３による利用者認証システムの利用者認証処理の別の手順を示すフローチャートである。

【０１０６】図１３のフローチャートにおいて、ステップＳ１３０１～Ｓ１３０３は、図１２のステップＳ１２０１～Ｓ１２０３と同様の内容なので、それらの説明は省略する。

【０１０７】ステップＳ１３０３において、ステップＳ１３０１において入力されたログイン名とステップＳ１３０２において入力されたパスワードを認証デーモン１１０２へ渡した後、ＯＳアカウントＤＢ１１０３のＯＳアカウント情報が利用可能か否かを判断する（ステップＳ１３０４）。ここで、ＯＳアカウント情報が利用可能な場合（ステップＳ１３０４肯定）は、実施の形態２による図９のステップＳ９０５へ移行する。

【０１０８】一方、ステップＳ１３０４において、ＯＳアカウント情報が利用可能でない場合（ステップＳ１３０４否定）は、つぎに、認証ＤＢ１１０８を用いてログイン名およびパスワードの検査をおこなう（ステップＳ１３０５）。以下、ステップＳ１３０５～Ｓ１３０９は、図１２のステップＳ１２０５～Ｓ１２０９と同様の内容なので、それらの説明は省略する。

【０１０９】以上説明したように、実施の形態３によれば、複数のＤＢから一つのＤＢを選択し、選択されたＤＢを用いて認証処理をおこなうので、複数のＤＢを選択的に用いるので、ＤＢの稼働率を向上させ、効率よく認証処理をすることができる。また、いずれかのＤＢが利用できない場合であっても、利用できるＤＢを用いて認証処理を確実におこなうことができる。

【０１１０】特に、複数のコンピュータシステムが任意の通信媒体を介して接続された分散環境において、特定のコンピュータシステムによって利用者情報を一元管理し、ログイン名およびパスワードにより利用者認証をおこない、分散環境上のサービスの利用を許可する利用者認証システムに対して有用である。

【０１１１】なお、実施の形態１から３で説明した利用者認証方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーション等のコンピュータで実行することにより実現される。このプログラムは、ハードディスク、フロッピーディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。またこのプログラムは、上記記録媒体を介してまたはネットワークを介して配布することができる。

【０１１２】

【発明の効果】以上説明したように、請求項１の発明によれば、ログイン名およびパスワードを含むＯＳアカウント情報を格納するＯＳアカウント情報格納手段と、前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報を用いて利用者の認証をおこなう第１認証手段と、前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報に基づいて、利用者認証情報を生成する生成手段と、前記生成手段により生成された利用者認証情報を格納する利用者認証情報格納手段と、前記利用者認証情報格納手段により格納された利用者認証情報を用いて利用者の認証をおこなう第２認証手段と、を備えているため、管理者に負担をかけることなく、システムのＯＳの認証と同様の認証をＷＷＷサーバー側でおこなうことができ、容易かつ確実に利用者認証をおこなうことができる利用者認証システムが得られるという効果を奏する。

【０１１３】また、請求項２の発明によれば、請求項１の発明において、前記第１認証手段または前記第２の認証手段のいずれかを選択する選択手段を備え、前記選択手段により選択された認証手段により認証をおこなうため、利用者が所望する認証方式を選択することができ、また、優先順位の高い認証方式による認証ができない場合に、つぎに優先順位の高い認証方式が選択されることにより、いずれかの認証方式に認証要求が集中しないようにし、効率的に認証処理をおこなうことができ、迅速かつ確実に利用者認証をおこなうことができる利用者認

証システムが得られるという効果を奏する。

【０１１４】また、請求項３の発明によれば、請求項２の発明において、前記選択手段が、複数の認証手段が選択可能である場合、前記第１認証手段を選択するため、迅速かつ確実に利用者認証をおこなうことができる利用者認証システムが得られるという効果を奏する。

【０１１５】また、請求項４の発明によれば、請求項１の発明において、前記第１の認証手段および／または前記第２の認証手段が、前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報または利用者認証情報格納手段により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうため、複数のＤＢから一つのＤＢを選択し、選択されたＤＢを用いて認証処理をおこなうので、複数のＤＢを選択的に用いるので、ＤＢの稼働率を向上させ、効率よく認証処理をすることができ、迅速かつ確実に利用者認証をおこなうことができる利用者認証システムが得られるという効果を奏する。ことを特徴とする。

【０１１６】また、請求項５の発明によれば、請求項４の発明において、前記第１の認証手段および／または前記第２の認証手段が、前記ＯＳアカウント情報格納手段により格納されたＯＳアカウント情報を用いることができないとき、前記利用者認証情報格納手段により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうため、いずれかのＤＢが利用できない場合であっても、利用できるＤＢを用いて認証処理をおこなうことができ、迅速かつ確実に利用者認証をおこなうことができる利用者認証システムが得られるという効果を奏する。

【０１１７】また、請求項６の発明によれば、ログイン名およびパスワードを含むＯＳアカウント情報を格納するＯＳアカウント情報格納工程と、前記ＯＳアカウント情報格納工程により格納されたＯＳアカウント情報を用いて利用者の認証をおこなう第１認証工程と、前記ＯＳアカウント情報格納工程よりに格納されたＯＳアカウント情報に基づいて、利用者認証情報を生成する生成工程と、前記生成工程により生成された利用者認証情報を格納する利用者認証情報格納工程と、前記利用者認証情報格納工程により格納された利用者認証情報を用いて利用者の認証をおこなう第２認証工程と、を含んでいるため、管理者に負担をかけることなく、システムのＯＳの認証と同様の認証をＷＷＷサーバー側でおこなうことができ、容易かつ確実に利用者認証をおこなうことができる利用者認証方法が得られるという効果を奏する。

【０１１８】また、請求項７の発明によれば、請求項６の発明において、前記第１認証工程により認証をおこなうかまたは前記第２の認証工程により認証をおこなうかを選択する選択工程を含み、前記選択工程により選択された認証工程により認証をおこなうことため、利用者が所望する認証方式を選択することができ、また、優先順位の高い認証方式による認証ができない場合に、つぎに優先順位の高い認証工程が選択されることにより、いずれかの認証工程に認証要求が集中しないようにし、効率的に認証処理をおこなうことができ、迅速かつ確実に利用者認証をおこなうことができる利用者認証方法が得られるという効果を奏する。

【０１１９】また、請求項８の発明によれば、請求項７の発明において、前記選択工程は、複数の認証工程により認証することが選択可能である場合、前記第１認証工程により認証するよう選択するため、迅速かつ確実に利用者認証をおこなうことができる利用者認証方法が得られるという効果を奏する。

【０１２０】また、請求項９の発明によれば、請求項６の発明において、前記第１認証工程および／または前記第２認証工程が、前記ＯＳアカウント情報格納工程により格納されたＯＳアカウント情報または利用者認証情報格納工程により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうことため、各工程における処理の稼働率を向上させ、効率よく認証処理をすることができ、迅速かつ確実に利用者認証をおこなうことができる利用者認証方法が得られるという効果を奏する。

【０１２１】また、請求項１０の発明によれば、請求項９の発明において、前記第１認証工程および／または前記第２認証工程は、前記ＯＳアカウント情報格納工程により格納されたＯＳアカウント情報を用いることができないとき、前記利用者認証情報格納工程により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうため、いずれかの工程による処理をおこなうことができない場合であっても、利用できる工程により認証処理をおこなうことができ、迅速かつ確実に利用者認証をおこなうことができる利用者認証方法が得られるという効果を奏する。

【０１２２】また、請求項１１の発明に係る記憶媒体は、請求項６～１０に記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムを機械読み取り可能となり、これによって、請求項６～１０の動作をコンピュータによって実現することが可能な記録媒体が得られるという効果を奏する。

【図面の簡単な説明】

【図１】この発明の実施の形態１による図書館情報管理システム全体の構成を示す説明図である。

【図２】実施の形態１による図書館情報管理システムの各サブシステムと図書館情報管理の業務との関係を示す説明図である。

【図３】実施の形態１による図書館情報管理システムのデータベースの構成を示す説明図である。

【図４】実施の形態１による図書館情報管理システムの図書管理サーバーのハードウエア構成を示すブロック図である。

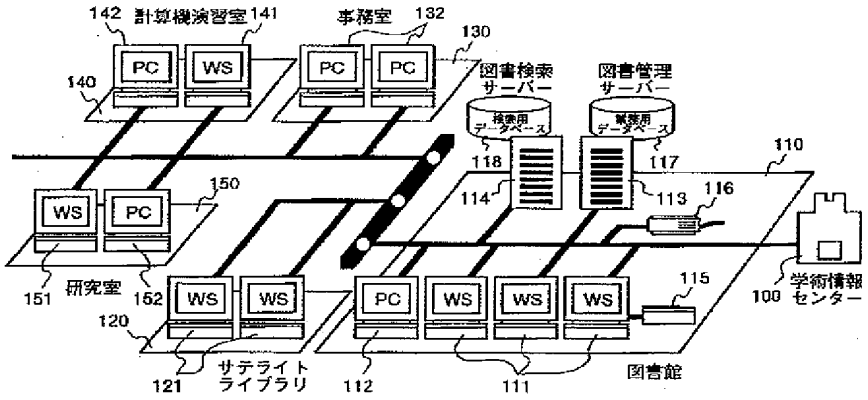
21

【図５】実施の形態１による利用者認証システムの構成を示す機能ブロック図である。
【図６】実施の形態１による利用者認証システムの認証情報生成処理の手順を示すフローチャートである。
【図７】実施の形態１による利用者認証システムの認証処理の手順を示すフローチャートである。
【図８】この発明の実施の形態２による利用者認証システムの構成を示す機能ブロック図である。
【図９】実施の形態２による利用者認証システムの認証処理の手順を示すフローチャートである。
【図１０】実施の形態２による利用者認証システムの認証方式選択部の選択処理の手順を示すフローチャートである。
【図１１】この発明の実施の形態３による利用者認証システムの構成を示す機能ブロック図である。
【図１２】実施の形態３による利用者認証システムの認証処理の手順を示すフローチャートである。
【図１３】実施の形態３による利用者認証システムの利用者認証処理の別の手順を示すフローチャートである。
【図１４】従来の利用者認証システムの構成を示す機能ブロック図である。
【符号の説明】
１００　学術情報センター
１１０　図書館
１１１，１２１，１４１，１５１　ワークステーション（ＷＳ）
１１２，１３２，１４２，１５２　パーソナルコンピュータ（ＰＣ）
１１３　図書管理サーバー
１１４　図書検索サーバー
１１７　業務用データベース
１１８　検索用データベース

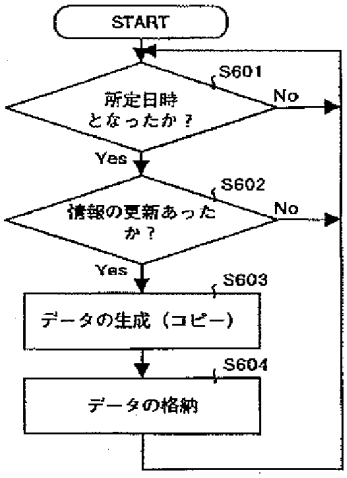
22

１２０　サテライトライブラリ
１３０　事務室
１４０　計算機演習室
１５０　研究室
２００　基本（目録管理）システム
２０１　図書検索システム
２０２　閲覧システム
２０３　発注受入システム
２０４　雑誌管理システム
２０５　蔵書点検システム
４０１　ＣＰＵ
４０５　ＨＤ
４０７　ＦＤ
４０８　ディスプレイ
４０９　インターフェイス（Ｉ／Ｆ）
４１０　通信回線
４１１　キーボード
４１２　マウス
４１３　スキャナ
４１４　バーコードリーダ
５００，８００，１１００　利用者
５０１，８０１，１１０１　ＣＵＩ／ＧＵＩ
５０２，８０２，１１０２　認証デーモン
５０３，８０３，１１０３　／ｅｔｃ／ｐａｓｓｗｄ（ＯＳアカウントＤＢ）
５０４，８０４，１１０４　ＷＷＷ
５０５，８０５，１１０５　ｈｔｔｐデーモン
５０６，８０６，１１０６　ＣＧＩ
５０７，８０７，１１０７　認証情報生成部
５０８，８０８，１１０８　認証ＤＢ
８１０　認証方式選択部

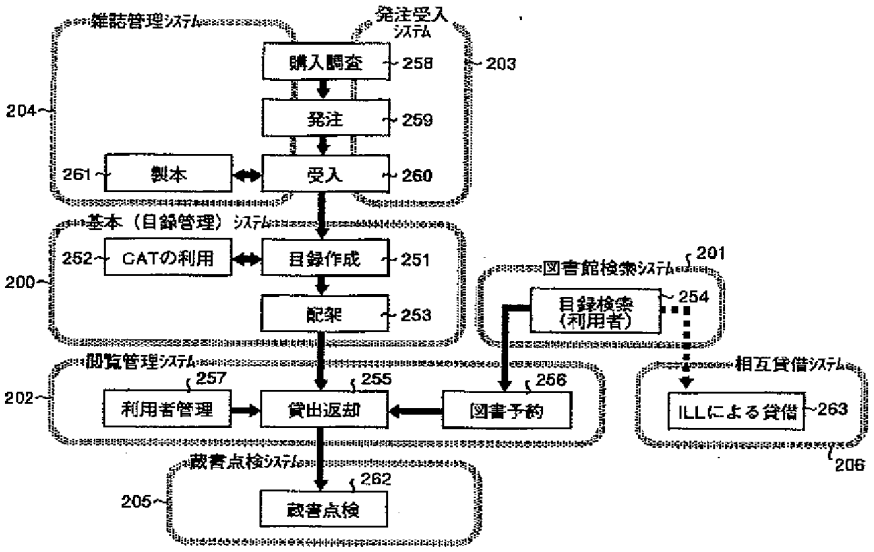
【図１】



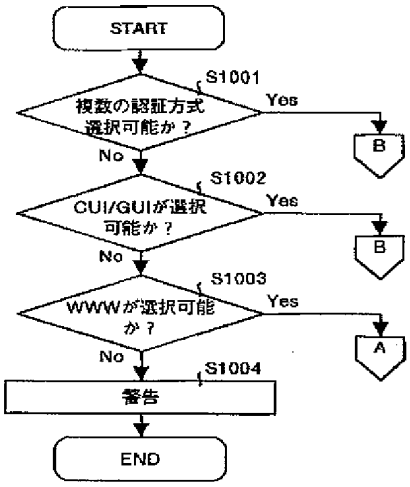
【図６】



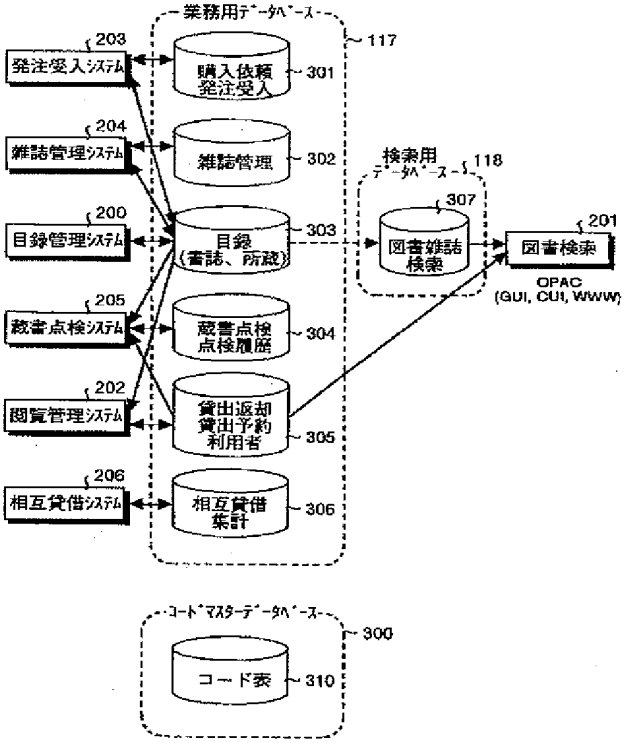
【図２】


雑誌管理システム
発注受入システム
購入調査
258
203
204
発注
259
261
製本
受入
260
基本（目録管理）システム
252
CATの利用
目録作成
251
200
配架
253
図書館検索システム
201
目録検索（利用者）
254
閲覧管理システム
257
255
256
202
利用者管理
貸出返却
図書予約
相互貸借システム
ILLによる貸借
263
206
蔵書点検システム
262
205
蔵書点検

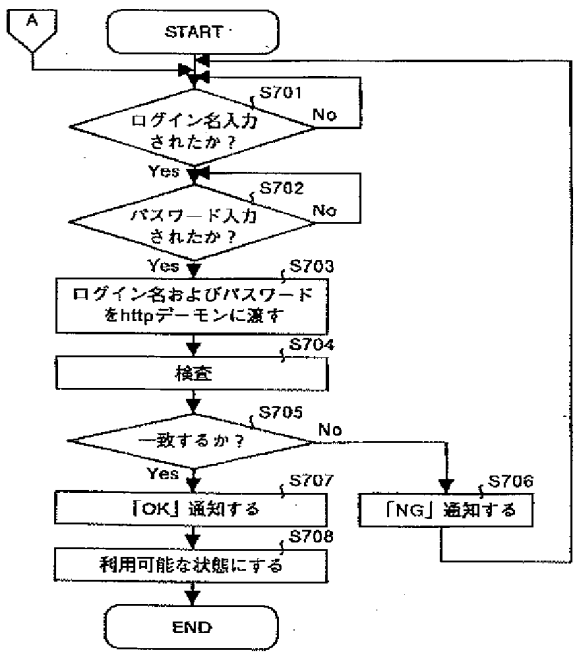
【図１０】


START
S1001
複数の認証方式選択可能か？
Yes
No
B
S1002
CUI/GUIが選択可能か？
Yes
No
B
S1003
WWWが選択可能か？
Yes
No
A
S1004
警告
END

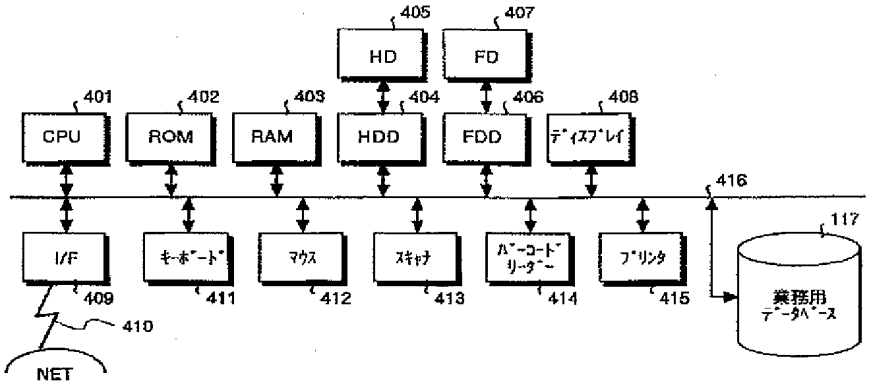
【図３】


業務用データベース
117
203
発注受入システム
購入依頼発注受入
301
204
雑誌管理システム
雑誌管理
302
200
目録管理システム
目録（書誌、所蔵）
303
検索用データベース
118
307
図書雑誌検索
201
図書検索
OPAC
(GUI, CUI, WWW)
205
蔵書点検システム
蔵書点検履歴
304
202
閲覧管理システム
貸出返却貸出予約利用者
305
206
相互貸借システム
相互貸借集計
306
コードマスターデータベース
300
コード表
310

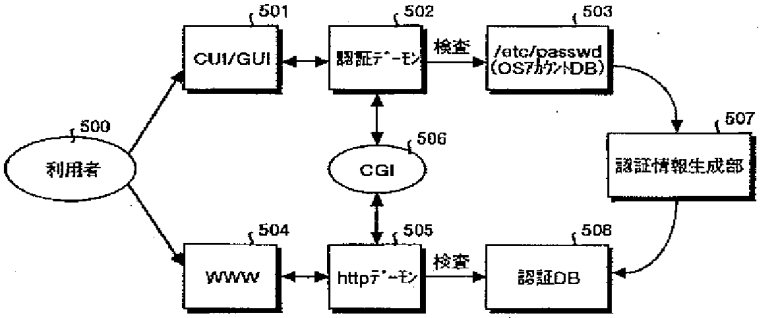
【図７】


A
START
S701
ログイン名入力されたか？
No
Yes
S702
パスワード入力されたか？
No
Yes
S703
ログイン名およびパスワードをhttpデーモンに渡す
S704
検査
S705
一致するか？
No
Yes
S707
「OK」通知する
S706
「NG」通知する
S708
利用可能な状態にする
END

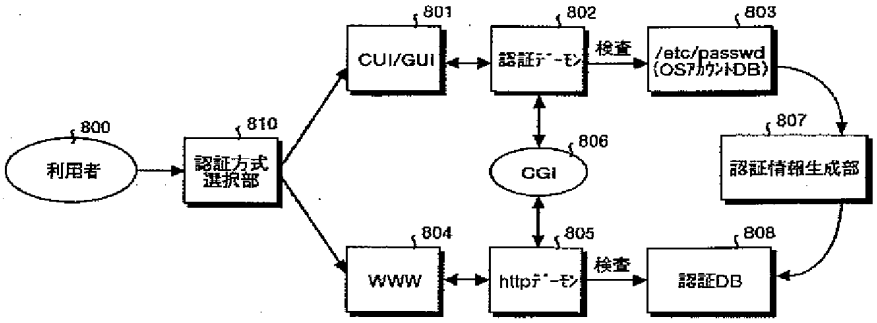
【図４】


405
HD
407
FD
401
CPU
402
ROM
403
RAM
404
HDD
406
FDD
408
ﾃﾞｨｽﾌﾟﾚｲ
416
I/F
409
410
NET
ｷｰﾎﾞｰﾄﾞ
411
ﾏｳｽ
412
ｽｷｬﾅ
413
ﾊﾞｰｺｰﾄﾞ ﾘｰﾀﾞｰ
414
ﾌﾟﾘﾝﾀ
415
117
業務用 ﾃﾞｰﾀﾍﾞｰｽ

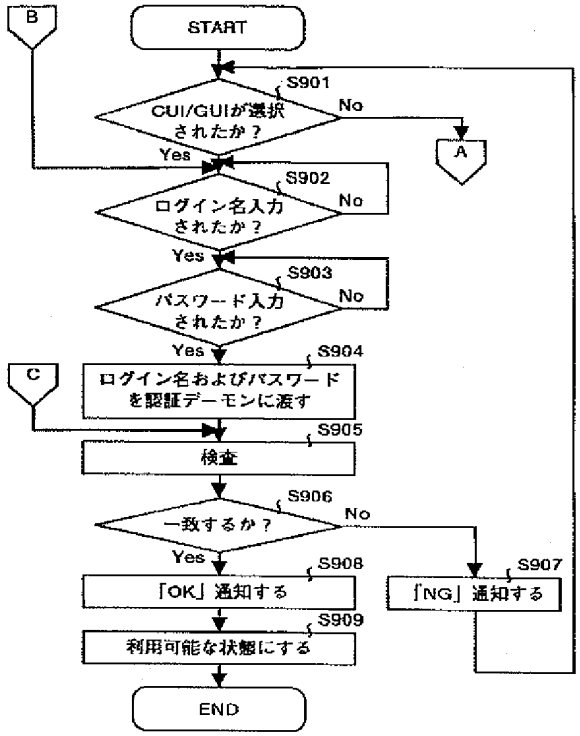
【図５】


501
CUI/GUI
502
認証ﾃﾞｰﾓﾝ
検査
503
/etc/passwd (OSｱｶｳﾝﾄDB)
500
利用者
506
CGI
507
認証情報生成部
504
WWW
505
httpﾃﾞｰﾓﾝ
検査
508
認証DB

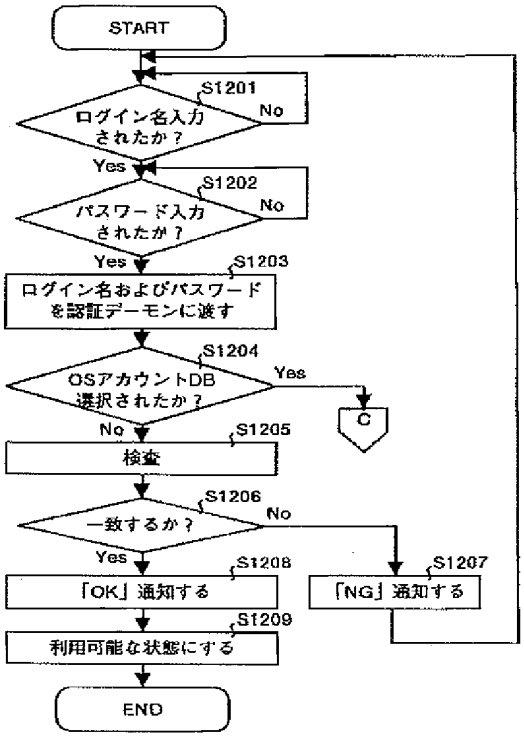
【図８】


801
CUI/GUI
802
認証ﾃﾞｰﾓﾝ
検査
803
/etc/passwd (OSｱｶｳﾝﾄDB)
800
利用者
810
認証方式 選択部
806
CGI
807
認証情報生成部
804
WWW
805
httpﾃﾞｰﾓﾝ
検査
808
認証DB

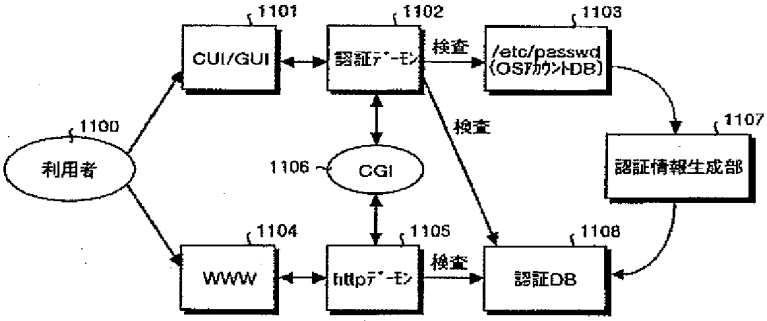
【図９】



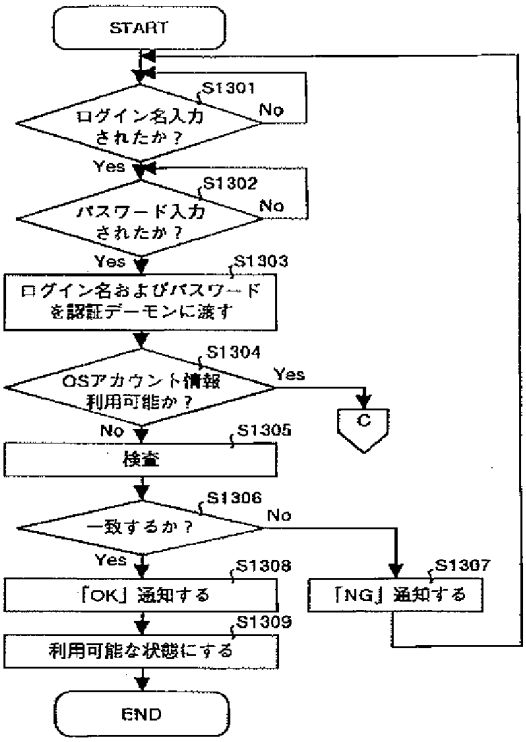
【図１２】



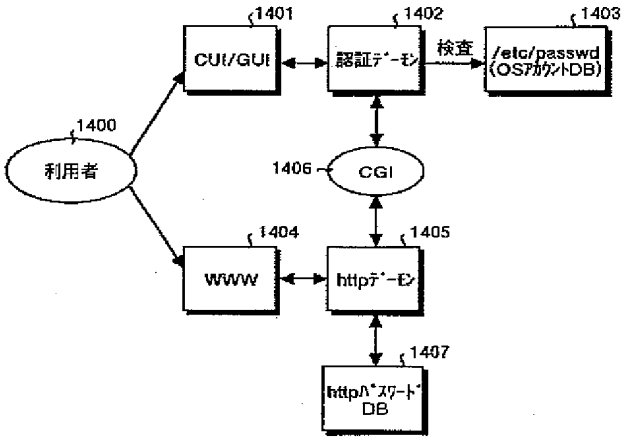
【図１１】



【図１３】



【図１４】


1401
1402
1403
CUI/GUI
認証ﾃﾞｰﾓﾝ
検査
/etc/passwd
(OSｱｶｳﾝﾄDB)
1400
利用者
1406
CGI
1404
1405
WWW
httpﾃﾞｰﾓﾝ
1407
httpﾊﾟｽﾜｰﾄﾞ
DB